The Origination message shall be is triggered when:

- a call or call leg originated by the intercept subject is routed toward a destination within the accessing system;
- a call or call leg originated by the intercept subject is routed toward a destination on an external public or private network;
- the destination number for a call or call leg originated by the intercept subject is translated from one set of digits to another. For example, speed number expansion or 800-number translation;
- a call was attempted that had no dialed digits (e.g., hot line), that was partially dialed, or that could not be completed by the accessing system; or
- a feature code was dialed or otherwise transmitted.

The Origination message includes the following parameters:

Table 5: **Origination Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call within a system. A unique call identity may be generated for the Origination message which is used to correlate other messages. An exception is possible when such an attempt is considered part of an on-going call (e.g., three-way calling or conference calling for some systems).
Calling PartyIdentity	C	Include, when more specific than the intercept subject identity associated with the CaseIdentity, to identify the originating number.
Called PartyIdentity	C	Include, when known to identify the called party. This shall not be present for calls that were partially dialed or could not be completed by the accessing system.
Input	M	Identifies specific user or translation input including when a call is attempted without input (e.g., hot line).
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
TransitCarrierIdentity	C	Include, when the transit network selection is known, to identify the transit carrier.
BearerCapability	C	Include, when known (or presumed), to indicate the requested bearer service for the origination.

See 6.3.5 "Origination Message" on page 46 for the Stage 3 description.

5.4.6 PacketEnvelope

The PacketEnvelope message is used to convey data packets over the CDC as they are intercepted. (Packet-mode communications delivered over CCCs or packet-mode communications using circuit-mode facilities do not use the PacketEnvelope.)

The PacketEnvelope message shall be triggered for the appropriate types of packet data services when:

- a packet-mode user communication intended for the intercept subject is detected; or
- a packet-mode user communication from the intercept subject is detected.

The PacketEnvelope message includes the following parameters:

Table 6: **PacketEnvelope Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Include when the packet is associated with a particular call instance.
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
Packet Information	M	
One of:		
ISDN- or ISUP-based user-to-user signaling information		Information pertaining to ISDN or ISUP user-to-user signaling messages.
IS-41-based short message service		Information pertaining to *IS-41* short message service messages.
GSM-based short message service		Information pertaining to GSM short message service messages.

See 6.3.6 "PacketEnvelope Message" on page 47 for the Stage 3 description.

5.4.7 Redirection

The Redirection message reports the redirection of a circuit-mode call.

The Redirection message shall be triggered when:

- an incoming call attempt to the intercept subject is forwarded (e.g. call forwarding or call diversion);
- an incoming call attempt to the intercept subject is deflected (e.g., call waiting deluxe or call deflection); or
- an incoming call attempt to an intercept subject with terminal or personal mobility is redirected to the intercept subject's current location (e.g., call delivery).

The Redirection message includes the following parameters:

Table 7: **Redirection Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call within a system.
Redirected-to PartyIdentity	M	Identifies the redirected-to party.
TransitCarrierIdentity	C	Included when the transit network selection is known to identify the transit carrier.
BearerCapability	C	Included when known (or presumed) to indicate the requested bearer service for the redirection.
System Identity	C	Included when a call to a wireless subscriber is redirected to another TSP and that identity is reasonably available.

See 6.3.7 "Redirection Message" on page 48 for the Stage 3 description.

5.4.8 Release

The Release message reports the release of the resources used for a circuit-mode call.

The Release message shall be triggered when:

- a circuit-mode call attempt is abandoned by the calling party; or
- a completed circuit-mode call is released.

The Release message includes the following parameters:

Table 8: **Release Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call within a system. The call identity is released (except for possible use by a CCClose message).
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
System Identity	C	Include, when a handed-off wireless call is released while being served by another TSP, to identify the last known TSP serving the subject.

See 6.3.8 "Release Message" on page 48 for the Stage 3 description.

5.4.9 ServingSystem

The ServingSystem message reports the TSP providing service to an intercept subject with terminal mobility, when the terminal is authorized for service.

A ServingSystem report shall be triggered when a mobile terminal is authorized for service with another TSP or in another service area.

The ServingSystem message includes the following parameters:

Table 9: **ServingSystem Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
SystemIdentity	C	Include, when authorizing service to a TSP, to identify the TSP.
NetworkAddress	C	Include, when available, to identify the redirect-to number of the base station (e.g., a personal or residential base station) providing service to the intercept subject.

See 6.3.9 "ServingSystem Message" on page 49 for the Stage 3 description.

5.4.10 TerminationAttempt

The TerminationAttempt message reports an incoming circuit-mode call attempt to the intercept subject. This message shall be sent regardless of the disposition of the call (e.g., busy, answered, redirected).

The TerminationAttempt message shall be triggered when:

- an incoming call to an intercept subject is detected; or
- a recall attempt involving the intercept subject is detected (e.g., hold recall, transfer recall, or attendant recall).

The TerminationAttempt message includes the following parameters:

Table 10: **TerminationAttempt Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call within a system. A unique call identity is generated for the TerminationAttempt message which is used to correlate other messages. An exception is possible when such an attempt is considered part of an on-going call (e.g., call waiting for some systems).
Calling PartyIdentity	M	Identifies the calling party to the extent known.
Called PartyIdentity	C	Include, when more specific than the subject identity associated with the CaseIdentity, to identify the called party.
BearerCapability	C	Include, when known (or presumed), to identify the requested bearer service.
RedirectedFromInformation	C	Include when the incoming call has information about previous redirection.

See 6.3.10 "TerminationAttempt Message" on page 49 for the Stage 3 description.

6 Stage 3 Description: Implementation Perspective

6.1 Protocol Definition

A protocol is defined in three basic aspects:

a. Transfer Syntax,

b. Transfer Semantics, and

c. Procedures.

The transfer syntax defines the messages passed between two functional entities. This definition may include various structures, but eventually defines the entire message structure down to the bit level. The syntax specifies the ways in which bits of messages are encoded for exchanging information between two functional entities.

The transfer semantics assigns meanings to the bits, bytes and structures of the transfer syntax. The exchanges of meanings allows the functional entities to share information and to act upon that information.

Procedures define the behavior of the functional entities. Procedures define which functional entities are allowed to initiate a particular transaction. Procedures define the possible responses to a given stimulus especially when dependent upon prior exchanges.

6.2 CDC Protocol Definition

6.2.1 CDC Underlying Data Transmission

The CDC messages defined by this Standard are an Open System Interconnection (OSI) Layer 7 or Application Layer protocol. The protocol for the CDC messages is called the Lawfully Authorized Electronic Surveillance Protocol (LAESP). The LAESP messages shall be delivered over CDCs employing a Standard or widely used data communication protocol.

6.2.2 CDC Parameter Encoding Objectives

The following are the objectives of the parameter encoding:

a. Allow flexible usage of the LAESP to transport a variety of information.

b. Provide a consistent and complete syntax for transferring information.

c. Facilitate implementation of message encoding and decoding software by using standardized techniques.

d. Allow as much syntactical checking as practical to be performed by the message parsers rather than deferring to the application.

e. Allow for parameter extension and modification throughout the life of the protocol.

6.2.3 CDC Syntax Definitions

The transferred information and messages are encoded to be binary compatible with *X.208 Abstract Syntax Notation One* (ASN.1) and the *X.209 Basic Encoding Rules* (BER).

These recommendations use precise definitions of the words *type*, *class*, *value*, and *parameter*. Those definitions are paraphrased here for clarity:

A *type*;, in the context of the abstract syntax or transfer syntax, is a set of all possible values. For example, an INTEGER is a type for all negative and positive integers.

A *class*, in the context of the abstract syntax or transfer syntax, is a one of four possible domains for uniquely defining a type. The classes defined by ASN.1 and BER are: UNIVERSAL, APPLICATION, CONTEXT, and PRIVATE. The UNIVERSAL class is reserved for international standards such as *X.208* and *X.209*. Most parameter type identifiers in the LAESP are encoded as CONTEXT specific class. Users of the LAESP may extend the protocol with PRIVATE class parameters without conflict with this Standard, but risk conflict with other users' extensions. APPLICATION class parameters are reserved by the LAESP Standard for future extensions.

A *value* is a particular instance of a type. For example, five (5) is a possible value of the type INTEGER.

A *parameter* in this Standard is a particular instance of the transfer syntax to transport a value consisting of a tag to identify the parameter type, a length to specify the number of octets in the value, and the value.

In the BER a *tag* (a particular type and class identifier) may either be a primitive or a constructor. A *primitive* is a pre-defined type (of class UNIVERSAL) and a *constructor* consists of other types (primitives or other constructors). A constructor type may either be *IMPLICIT* or *EXPLICIT*. An *IMPLICIT* type is encoded with the constructor identifier alone. Both ends of a communication must understand the underlying structure of the IMPLICIT types. *EXPLICIT* types are encoded with the identifiers of all the contained types. For example, an IMPLICIT Number of type INTEGER would be tagged only with the "Number" tag, where an EXPLICIT Number of type INTEGER would have the INTEGER tag within the Number tag. This Standard uses IMPLICIT tagging for more compact message encoding. Parameters of the CHOICE type are encoded EXPLICIT to ensure compatibility with various ASN.1 versions and compilers.

6.3 CDC Message Definitions

The LAESMessage parameter defines the LAES messages.

```
Laesp DEFINITIONS IMPLICIT TAGS ::=
BEGIN

LAESMessage ::= CHOICE {
        answer          [1] Answer,
        ccClose         [2] CCClose,
        ccOpen          [3] CCOpen,
        change          [4] Change,
        origination     [5] Origination,
        packetEnvelope  [6] PacketEnvelope,
        redirection     [7] Redirection,
        release         [8] Release,
        servingSystem   [9] ServingSystem,
        termAttempt     [10] TerminationAttempt
--      connTest        [11] ConnectionTest     - - see annex E
}
```

6.3.1 Answer Message

The Answer message is used to report that a connection-oriented call or leg has been answered.

```
Answer ::= SEQUENCE {
                [0] CaseIdentity,
                [1] IAPSystemIdentity           OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that system.
                [2] TimeStamp,
                [3] CallIdentity,
answering       [4] PartyIdentity               OPTIONAL,
                -- include, when known, to identify the answering party or agent (and the
                -- terminal used).
                [5] Location                    OPTIONAL,
                -- Include, when a terminating call is answered, the location
                -- information is reasonably available to the IAP and delivery is
                -- authorized, to identify the location of an intercept subject's
                -- mobile terminal
                [6] EXPLICIT BearerCapability   OPTIONAL
                -- include, when known (or presumed), to indicate the granted bearer
                -- capability.
}
```

See 5.4.1 "Answer" on page 32 for the Stage 2 description.

6.3.2 CCClose Message

The CCClose message is used to report the end of call content delivery on the CCC.

```
CCClose ::= SEQUENCE {
                [0] CaseIdentity,
                [1] IAPSystemIdentity   OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that system.
                [2] TimeStamp,
                [3] CallIdentity        OPTIONAL,
                -- include for circuit-mode intercepts
                [4] EXPLICIT CCCIdentity
}
```

See 5.4.2 "CCClose" on page 33 for the Stage 2 description.

6.3.3 CCOpen Message

The CCOpen message is used to report the beginning of call content delivery on the CCC.

```
CCOpen ::= SEQUENCE {
                [0] CaseIdentity,
                [1] IAPSystemIdentity   OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that system.
                [2] TimeStamp,
                CHOICE {
                        [3] CallIdentity,       -- for circuit-mode intercepts
                        [4] PDUType             -- for packet-mode intercepts
                },
                [5] EXPLICIT CCCIdentity
}
```

See 5.4.3 "CCOpen" on page 34 for the Stage 2 description.

6.3.4 Change Message

The Change message is used to report merging or splitting of connection-oriented call identities.

```
Change ::= SEQUENCE {
                [0] CaseIdentity,
                [1] IAPSystemIdentity   OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that system.
                [2] TimeStamp,
previous        [3] SEQUENCE OF CallIdentity, -- previous call identities
resulting       [4] SEQUENCE OF SEQUENCE { -- resulting calls
                        [0] CallIdentity,
                        [1] EXPLICIT CCCIdentity        OPTIONAL
                        -- included when the contents of the resulting call are delivered
                        -- to identity the CCC(s) in the resulting call.
                }
}
```

See 5.4.4 "Change" on page 35 for the Stage 2 description.

6.3.5 Origination Message

The Origination message reports authorized connection-oriented call origination attempts or number translations for the intercept subject performed by the Access Function.

```
Origination ::= SEQUENCE {
                [0] CaseIdentity,
                [1] IAPSystemIdentity   OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that system.
                [2] TimeStamp,
                [3] CallIdentity,
calling         [4] PartyIdentity               OPTIONAL,
                -- include, when more specific than the subject identity associated
                -- with the CaseIdentity, to identify the calling number
called          [5] PartyIdentity               OPTIONAL,
                -- include if known
input           CHOICE {
userInput               [6] VisibleString (SIZE (1..32)),
                        -- use if input is known to be from the user
                        -- e.g., "12025551234" or "*123"
translationInput        [7] VisibleString (SIZE (1..32))
                        -- use for inputs to translation
                        -- e.g., "12025551234" or "*123"
                },
                [8] Location                    OPTIONAL,
                -- Include, when the location information is reasonably available to
                -- the IAP and delivery is authorized, to identify the location of an
                -- intercept subject's mobile terminal
                [9] TransitCarrierIdentity      OPTIONAL,
                -- include if known
                [10] EXPLICIT BearerCapability  OPTIONAL
                -- include if known (or presumed)
}
```

See 5.4.5 "Origination" on page 35 for the Stage 2 descrition.

6.3.6 PacketEnvelope Message

The PacketEnvelope message delivers intercepted packets to an LEA.

```
PacketEnvelope ::= SEQUENCE {
                        [0] CaseIdentity,
                        [1] IAPSystemIdentity   OPTIONAL,
                        -- include to identify the system containing the Intercept Access
                        -- Function when the underlying data carriage does not imply
                        -- that system.
                        [2] TimeStamp,
                        [3] CallIdentity        OPTIONAL,
                        [4] Location            OPTIONAL,
                        -- Include, when the location information is reasonably available
                        -- to the IAP and delivery is authorized, to identify the
                        -- location of an intercept subject's mobile terminal
packetInformation       CHOICE {
iSDNUserToUserSignaling         [5] SEQUENCE {
callIdentity                            [0] CallIdentity,
sending                                 [1] PartyIdentity,
interceptedUUPacket                     [2] OCTET STRING (SIZE (1..127))
                                },

is41ShortMessageService         [6] SEQUENCE {
originalOriginatingAddress              [0] PartyIdentity,
originalDestinationAddress              [1] PartyIdentity,
originatingAddress                      [2] PartyIdentity       OPTIONAL,
                                        -- include if known and different than the
                                        -- originalOriginatingAddress
destinationAddress                      [3] PartyIdentity       OPTIONAL,
                                        -- include if known and different than the
                                        -- originaldestinationAddress
smsTeleserviceIdentifier                [4] INTEGER (-32768..32767),--see IS-41
interceptedISSMSPacket                  [5] OCTET STRING (SIZE (1..255))
                                },

gsmSMShortMessageService        [7] SEQUENCE {
senderAddress                           [0] PartyIdentity,
receiverAddress                         [1] PartyIdentity,
interceptedGSMSMSPacket                 [2] OCTET STRING (SIZE (1..255))
                                }
                        }
}
```

See 5.4.6 "PacketEnvelope" on page 37 for the Stage 2 descrition.

6.3.7 Redirection Message

The Redirection message indicates that an incoming connection-oriented call attempt, originally directed toward a subject, has been redirected by the subject.

```
Redirection ::= SEQUENCE {
                [0] CaseIdentity,
                [1] IAPSystemIdentity   OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that system.
                [2] TimeStamp,
                [3] CallIdentity,
redirectedTo    [4] PartyIdentity,
                [5] TransitCarrierIdentity      OPTIONAL,
                -- include if known
                [6] EXPLICIT BearerCapability   OPTIONAL,
                -- include if known (or presumed)
systemIdentity  [7] VisibleString (SIZE (1..15))        OPTIONAL
                -- include when a call to a wireless subscriber is redirected to another
                -- TSP and that identity is reasonably available.
                -- e.g., "MSCID-12345-123" or "2025551234"
}
```

See 5.4.7 "Redirection" on page 38 for the Stage 2 descrition.

6.3.8 Release Message

The Release message is used to report that a connection-oriented call has been released.

```
Release ::= SEQUENCE {
                [0] CaseIdentity,
                [1] IAPSystemIdentity   OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that system.
                [2] TimeStamp,
                [3] CallIdentity,
                [4] Location                    OPTIONAL,
                -- Include, when the location information is reasonably available to
                -- the IAP and delivery is authorized, to identify the location of an
                -- intercept subject's mobile terminal
systemIdentity  [5] VisibleString (SIZE (1..15))OPTIONAL
                -- include, when a handed-off wireless call is released while being
                -- served by another TSP to identify the last known TSP serving the
                -- subject, e.g., "MSCID-12345-123" or "2025551234"
}
```

See 5.4.8 "Release" on page 39 for the Stage 2 descrition.

6.3.9 ServingSystem Message

The ServingSystem message is used to report a change in the current TSP or service area for terminal or personal mobility.

```
ServingSystem ::= SEQUENCE {
                  [0] CaseIdentity,
                  [1] IAPSystemIdentity                    OPTIONAL,
                  -- include to identify the system containing the Intercept Access
                  -- Function when the underlying data carriage does not imply that system.
                  [2] TimeStamp,
systemIdentity    [3] VisibleString (SIZE (1..15))        OPTIONAL,
                  -- include, when authorizing service to a TSP, to identify the TSP
                  -- e.g., "MSCID-12345-123" or "2025551234"
networkAddress    [4] VisibleString (SIZE (1..15))        OPTIONAL
                  -- include if the serving TSP can only be identified by
                  -- a redirect-to number e.g., a personal or residential base station
                  -- directory number "2025551234"
}
```

See 5.4.9 "ServingSystem" on page 40 for the Stage 2 descrition.

6.3.10 TerminationAttempt Message

The TerminationAttempt message is used to report a connection-oriented call termination attempt.

```
TerminationAttempt ::= SEQUENCE {
                  [0] CaseIdentity,
                  [1] IAPSystemIdentity                    OPTIONAL,
                  -- include to identify the system containing the Intercept Access
                  -- Function when the underlying data carriage does not imply that system.
                  [2] TimeStamp,
                  [3] CallIdentity,
calling           [4] PartyIdentity,
called            [5] PartyIdentity                        OPTIONAL,
                  -- include, when more specific than the subject identity associated
                  -- with the CaseIdentity, to identify the called party.
                  [6] EXPLICIT BearerCapability            OPTIONAL,
                  -- included when known (or presumed)
                  [7] RedirectedFromInformation            OPTIONAL
                  -- include if this termination attempt is a result of a redirected call
}
```

See 5.4.10 "TerminationAttempt" on page 41 for the Stage 2 descrition.

6.4 CDC Parameter Definitions

6.4.1 BearerCapability

The BearerCapability parameter indicates a requested or granted bearer service.

```
BearerCapability ::= CHOICE {
        speech                  [0] NULL,
        f3100HzAudio            [1] NULL,
        bearerCapInfoElement    [2] OCTET STRING (SIZE (1..64))
                -- encoded according to T1.607 Bearer Capability information
                -- element starting with octet 3
}
```

6.4.2 CallIdentity

The CallIdentity parameter is used to uniquely identify a particular call within the context of a single system. The CCOpen, CCClose, and Change message can correlate the CallIdentity to one or more CCCs when content is delivered. A CallIdentity may be created with a CCOpen, Origination, TerminationAttempt or Change message. A CallIdentity may be released for other uses with a CCClose, Release or Change message. Special consideration may be needed for the CCOpen and CCClose usages, so that the CallIdentity is not prematurely released with the Release message. HLRs and similar systems that do not correlate messages with CallIdentity(ies) do not need to release the CallIdentity.

```
CallIdentity ::= SEQUENCE {
sequenceNumber          [0] VisibleString (SIZE (1..25)),
systemIdentity          [1] VisibleString (SIZE (1..15))        OPTIONAL
                        -- include when the system issuing the sequenceNumber is
                        -- different than the accessing system.
                        -- e.g., CLLI code, "MSCID-12345-123" or "2025551234" (E.164
                        -- address of node)
}
```

6.4.3 CaseIdentity

The CaseIdentity parameter contains a case identity assigned by the LEA for a particular electronic surveillance. The CaseIdentity will be designated by the LEA and provided to a TSP at the time of provisioning of an electronic surveillance.

```
CaseIdentity ::= VisibleString (SIZE (1..25))
                -- e.g., "FBI-12345" or "NYPD-12345"
```

6.4.4 CCCIdentity

The CCCIdentity parameter identifies the CCC or pair of CCCs used for conveying call content. Each CCC is identified with a VisibleString which may contain a directory number (e.g., "202-555-1111"), a trunk identity (e.g., "FBITG-001" or "LAES-999"), an IP network address (e.g., "IP: 101.012.103.104:100") or an X.25 network address (e.g., "X121: 1234-5678901234").

```
CCCIdentity ::= CHOICE {
combCCC         [0] VisibleString (SIZE (1..20)),       -- combined CCC
sepCCCpair      [1] SEQUENCE {                          -- separated CCC
sepXmitCCC              [0] VisibleString (SIZE (1..20)), -- transmit path
                        -- (from the intercept subject or redirected-to party)
sepRecvCCC              [1] VisibleString (SIZE (1..20)) -- receive path
                        -- (to the intercept subject or redirected-to party)
                },
indXmitCCC      [2] VisibleString (SIZE (1..20)), -- individual transmit path
                -- (from the intercept subject or redirected-to party)
indRecvCCC      [3] VisibleString (SIZE (1..20)), -- individual receive path
                -- (to the intercept subject or redirected-to party)
indCCC          [4] VisibleString (SIZE (1..20)) -- individual CCC without
                -- a specified direction. Use only in CCClose messages.
}
```

6.4.5 IAPSystemIdentity

The IAPSystemIdentity parameter identifies the system of the Intercept Access Point and should not imply the specific location of an intercept subject.

```
IAPSystemIdentity ::= VisibleString (SIZE (1..15))
        -- e.g., CLLI code, "MSCID-12345-123" or "2025551234" (E.164 address of node)
```

6.4.6 Location

The Location parameter provides location information about the subject's mobile terminal.

```
Location ::= VisibleString (SIZE (1..32))        -- e.g., "WESTGATE" or "CELL017"
```

6.4.7 PartyIdentity

The PartyIdentity parameter identifies a party to a call or call attempt.

```
PartyIdentity ::= SEQUENCE {
                        -- include those identification elements necessary to uniquely
                        -- identify the party known at the point in call and are
                        -- authorized. At least one of the following parameters is
                        -- required.

                        -- * denotes nature of number is required to interpret

esn                     [0] VisibleString (SIZE (8))                    OPTIONAL,
                        -- AMPS-based Electronic Serial Number
                        -- a hexadecimal string e.g., "82ABCDEF"
imei                    [1] VisibleString (SIZE (1..15))                OPTIONAL,
                        -- GSM-based International Mobile Equipment Identity
tei                     [2] VisibleString (SIZE (1..15))                OPTIONAL,
                        -- ISDN-based Terminal Equipment Identity
spid                    [3] VisibleString (SIZE (3..20))                OPTIONAL,
                        -- ISDN-based Service Profile Identifier
imsi                    [4] VisibleString (SIZE (1..15))                OPTIONAL,
                        -- International Mobile Station Identity
                        -- E.212 number beginning with Mobile Country Code
min                     [5] VisibleString (SIZE (10))                   OPTIONAL,
                        -- AMPS-based Mobile Identification Number
dn                      [6] VisibleString (SIZE (1..15))                OPTIONAL,
                        -- e.g., called directory number or network provided calling
                        -- number.
userProvided            [7] VisibleString (SIZE (1..15))                OPTIONAL,
                        -- user provided calling number as supplied
appearanceId            [8] VisibleString (SIZE (1..15))                OPTIONAL,
                        -- include for instruments or services with multiple line,
                        -- station, or call appearances
callingCardNum          [9] VisibleString (SIZE (1..20))                OPTIONAL,
ipAddress               [10] VisibleString (SIZE (1..32))               OPTIONAL,
                        -- decimal quad notation e.g., "123.123.123.123" (not a URL)
x121                    [11] VisibleString (SIZE (1..15))               OPTIONAL,
                        -- begin with DNIC
trunkId                 [12] VisibleString (SIZE (1..32))               OPTIONAL,
                        -- indicate trunk group, trunk number or both
                        -- This is usually used to identify an associate when other
                        -- identifying information is not available.
```

```
                        -- This may also identify a subject's agent (e.g., screening
                        -- service).
subaddress              [13] OCTET STRING (SIZE (2..14))              OPTIONAL,
                        -- encoded according to T1.607 Subaddress information element
                        -- starting with octet 3
genericAddress          [14] SEQUENCE OF VisibleString (SIZE (1..32))  OPTIONAL,
                        -- indicate use of the generic address
genericDigits           [15] SEQUENCE OF VisibleString (SIZE (1..32))  OPTIONAL,
                        -- indicate use of the generic digits
genericName             [16] SEQUENCE OF VisibleString (SIZE (1..48))  OPTIONAL,
                        -- indicate use of the generic name
port                    [17] VisibleString (SIZE (1..32))             OPTIONAL,
                        -- identify a particular equipment port.
                        -- This is used to identify an associate when other
                        -- identifying information is not available.
context                 [18] VisibleString (SIZE (1..64))             OPTIONAL,
                        -- identify the context and special considerations of the
                        -- supplied identifier(s), especially when the identifier(s)
                        -- is(are) abnormal (e.g., international, private, restricted,
                        -- operator, no address, hotel/motel, coin, etc.
isdnHighLayer           [19] OCTET STRING (SIZE (2..14))              OPTIONAL,
                        -- include if known
                        -- encoded according to T1.607 High Layer Compatibility
                        -- information element starting with octet 3
isdnLowLayer            [20] OCTET STRING (SIZE (2..14))              OPTIONAL
                        -- include if known
                        -- encoded according to T1.607 Low Layer Compatibility
                        -- information element starting with octet 3
}
```

6.4.8 PDUType

The PDUType parameter indicates the intercepted packet type on a CCC. Negative values are reserved for bilateral agreement or protocol extension.

```
PDUType ::= ENUMERATED {
        isdnBchannel    (0),    -- see BearerCapability parameter
        isdnDchannel    (1),    -- intermixed Q.931, Q.932, and X.25
        ip              (2),    -- Internet protocol packets
        ppp             (3),    -- Internet point-to point protocol packets
        x25             (4)     -- X.25 LAPB packets
}
```

6.4.9 RedirectedFromInformation

The *RedirectedFromInformation parameter is used to report information* about the last redirecting party and the original redirecting party on calls that are redirected to the subject.

```
RedirectedFromInformation ::= SEQUENCE {
lastRedirecting         [0] PartyIdentity                   OPTIONAL,
                        -- include if known
originalCalled          [1] PartyIdentity                   OPTIONAL,
                        -- include if known
numRedirections         [2] INTEGER (1..100)                OPTIONAL
                        -- include if known
}
```

6.4.10 TimeStamp

The TimeStamp parameter identifies the date and time of access.

```
TimeStamp ::= GeneralizedTime
```

6.4.11 TransitCarrierIdentity

The TransitCarrierIdentity parameter identifies an interexchange carrier.

```
TransitCarrierIdentity ::= VisibleString (SIZE (3..7))
                -- the carrier access code (if applicable) and carrier identification
                -- code e.g., "123" or "10123" or "1012345" or "9501234"
END
```

6.5 CCC Protocols

6.5.1 CCC Encoding for Circuit-Mode Services

Call content shall be encoded on CCCs using a standard or widely used network bearer services. The intercepted content shall be delivered without modifying the content within the quality objectives for the intercepted network bearer service. Speech and 3.1 kHz audio bearer services using digital facilities shall use the μ-law encoding of ITU-T Recommendation G.711, *Pulse code modulation (PCM) of voice frequencies* .

Signaling on the CCC or out-of-band signaling may be used to inform the LEA when call content is being delivered.

6.5.2 CCC Encoding for Packet-Mode Services

Intercepted packet-mode data communications shall be delivered to an LEA when a CCC is used by forwarding the intercepted Protocol Data Units (PDUs) employing a standard or widely used protocol. The intercepted PDUs shall include sufficient addressing information to associate the PDU with the parties of the communication. The intercepted PDUs shall be delivered without modification, except for possible re-framing, segmentation, or enveloping required to transport the information to the Collection Function.

The choice of packet delivery protocol is determined at the time that the intercept is provisioned. This delivery method remains in effect until changed by subsequent provisioning.

6.6 LAESP Compatibility Guidelines

The guidelines ensure that there is no long term impediment to the evolution of networks and the implementation of significant new functionality.

6.6.1 Guidelines For Forward Compatibility

When developing a new protocol or enhancing an existing protocol, it is important to remember that a node using one version of protocol may, in the future, need to communicate with nodes using the enhanced version of the basic protocol. Hence, the protocol should be easy to enhance (e.g., easy to add new optional parameters). In addition, procedures should be built into the existing protocol to handle the situations when new messages, known messages with unknown parameters, or known parameters with unknown codes are received.

All revisions of this Standard shall contain a mechanism for forward compatibility. The following list contains the basic requirements of the mechanism:

a. When the LAESP message is received and it contains all the required parameters, the additional parameters in the received message, known or unknown, may be ignored. The received message should not be

rejected because of the unknown parameters in it. In cases that the received message should be relayed to another node, the additional parameters should be passed unchanged.

b. For existing protocols, state the action to be taken on receipt of spare or reserved values of defined parameters (e.g., treat as appropriate default values, transmit them unchanged at the intermediate nodes, and ignore them at the end nodes).

c. State that all new messages shall have the ability to add new optional fields.

d. Unallocated codes of defined fields should be examined and handled as either spare codes or a default code.

6.6.2 Guidelines For Backward Compatibility

When enhancing an existing protocol, it is important to keep in mind that a node using one version of a protocol may need to communicate with nodes using older versions of the same protocol. Hence, the protocol should not be changed abruptly into a form which the earlier protocol versions cannot even interpret. For example, one should not change a fixed length mandatory parameter to an optional parameter in an existing message.

All revisions of this Standard shall contain a mechanism for backward compatibility. The following list contains the basic guidelines to be included.

6.6.2.1 Existing Messages

a. The ability of receiving any existing messages shall be possible, since the removal of a message implies the removal of a function.

b. The effect of receiving any existing message, parameter, or function in a new version, must be the same as that in previous versions. The effects of new parameters or parameter values will thus be purely additive.

6.6.2.2 Parameters in Existing Messages

Message parameters in the Parameter Set consist of 2 basic types, mandatory and optional, and need not occur in a pre-defined order. All mandatory and optional parameters have variable length, although some parameters may have their length restricted.

The following guidelines shall apply:

a. Optional parameters shall not become mandatory.

b. Mandatory parameters shall not become optional.

c. Additional mandatory parameters shall not be added to an existing message.

d. Additional optional parameters can be added to an existing message.

e. Existing mandatory parameters shall not be removed from existing messages.

f. The range of any parameter for an existing message shall not be reduced.

g. The meaning of any defined parameter value shall not be changed on an existing message.

h. There are no restrictions on the parameters for new messages.

i. The sequence of parameters in an existing SEQUENCE type shall not be changed.

j. New parameters may be added to the end of an existing SEQUENCE type. (The value of the parameter identifiers used may be in any order to allow addition of existing parameters to an existing SEQUENCE type.)

k. New parameters may be added to an existing CHOICE type, unless the CHOICE is mandatory.

6.6.2.3 New Messages

New messages may be added after a Standard has been published; however, nodes that do not recognize these new messages will ignore them, internally indicating that the information was not recognized.

6.6.2.4 New Parameters

New optional parameters can be added to existing messages after a Standard has been published; however, nodes that do not recognize these new parameters may ignore them.

6.6.2.5 New Parameter Fields

New fields may be added to, or spare fields may be used in existing parameters; however, nodes that do not recognize these new fields may ignore these fields.

6.6.2.6 New Parameter Values

Previously spare, reserved, or unallocated parameter values can be used. These will be treated at the receiving node as defined in Item b of Section 6.6.1.

Annex A Deployment Examples

This Annex is informative and is not considered part of this Standard.

A.1 Possible Network Deployment of IAPs

IAPs may be implemented at a variety of points within a network, depending on the particular telecommunication equipment's architecture, the features and services that are being monitored, and the impact the monitoring at the selected point may have on normal call operation. Generally, it may be assumed that the primary location of the major IAPs are located in the network equipment shown in Table 11.

Table 11: **IAP Primary Locations**

IAP	Primary Equipment Location
CIAP	Circuit-mode switch
IDIAP	Circuit-mode or packet-mode switch
PDIAP	Packet-mode switch
SSIAP	Home Location Register

It is, however, possible to locate these IAPs within other types of equipment. It should be understood that an IAP placed in a node not corresponding to the primary type of equipment may provide reduced functionality.

For land line subscribers Figure 11 depicts a possible deployment where the access points are in several different pieces of equipment.

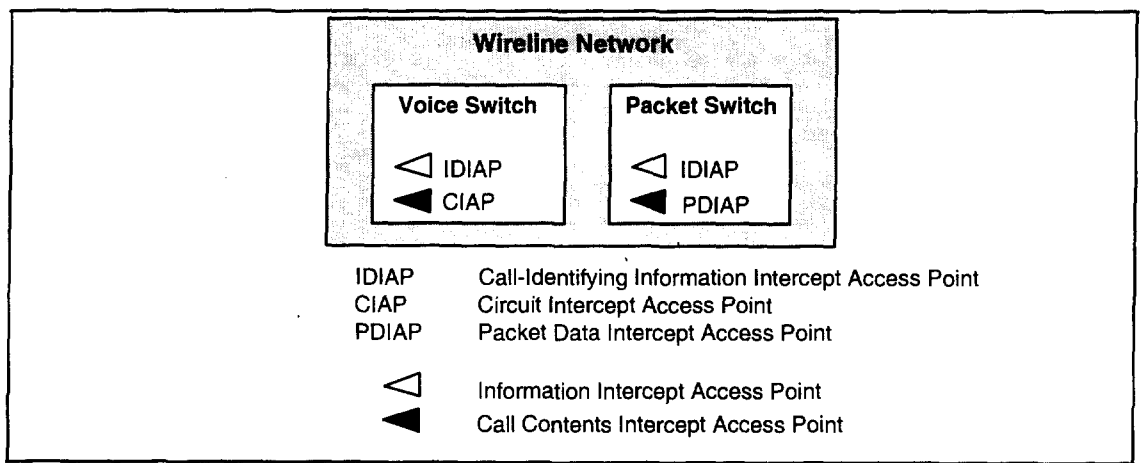

Figure 11: **Land Line IAPs**

Mobile telephony is more complex. The IAPs for a given intercept subject may be spread across several different clusters of equipment. There is a cluster of equipment at the intercept subject's home and there is another cluster of equipment around the system providing service to the intercept subject. These two clusters may be one and the same, but the more general

problem is when they are separate. Indeed for some TSPs, these clusters are always separated.

Figure 12 shows possible IAPs deployed in a mobile intercept subject's home equipment cluster.

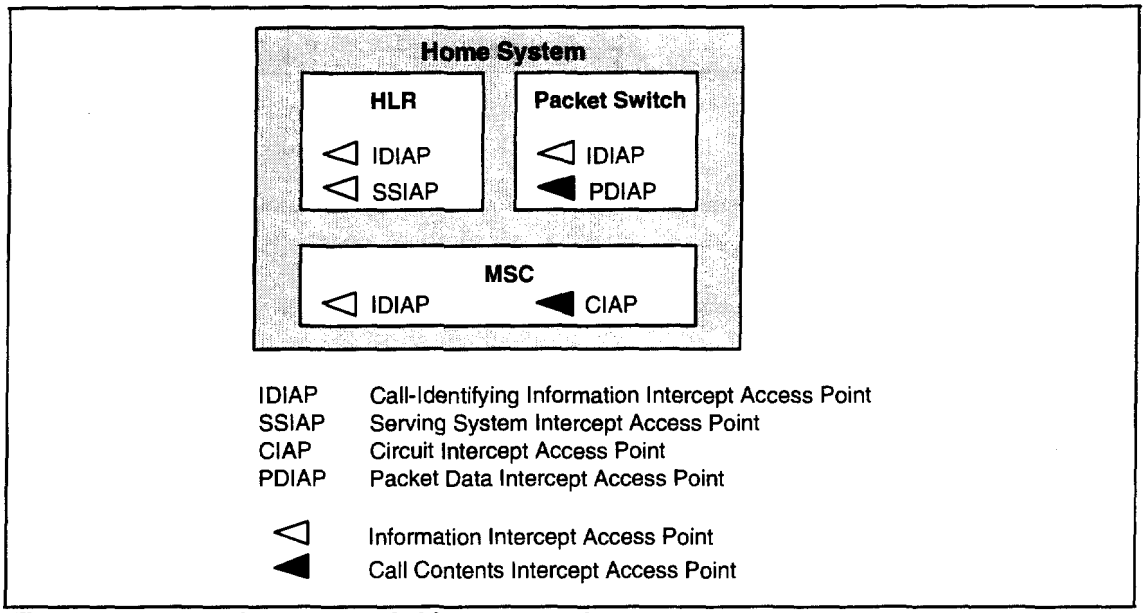

Figure 12: **Mobile Intercept Subject's Home System IAPs**

Figure 13 shows possible IAPs deployed in a mobile intercept subject's Serving System equipment cluster.

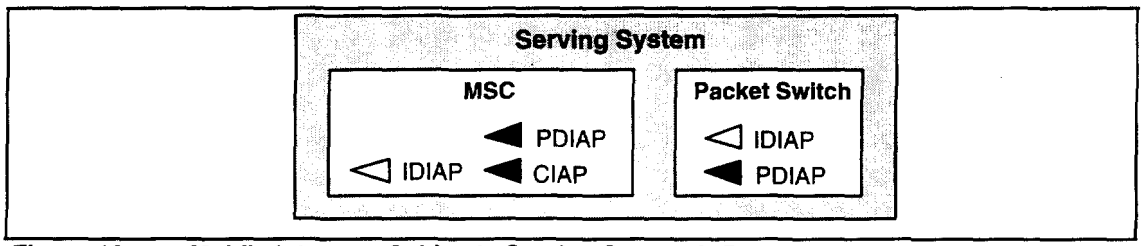

Figure 13: **Mobile Intercept Subject's Serving System IAPs**

When the Redirecting System is a system other than the intercept subject's Home System, it may be desirable to access all of these Redirecting Systems to gain access to the call content of calls intended for the intercept subject. Figure 14 shows possible IAPs.

A.2 Access and Delivery Function Equipment Configuration

There are several switching equipment configurations possible for intercept functions.

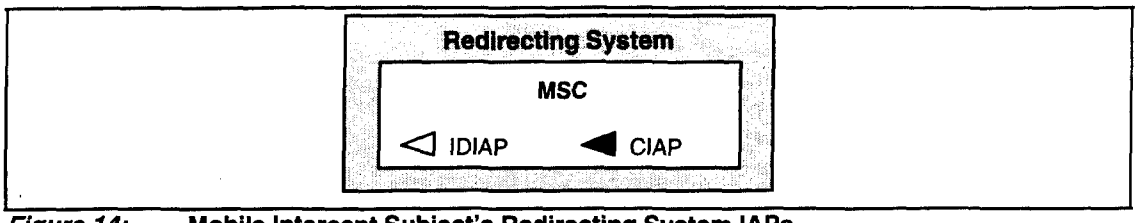

Figure 14: **Mobile Intercept Subject's Redirecting System IAPs**

One method is to use an external Delivery Function as shown in Figure 15.

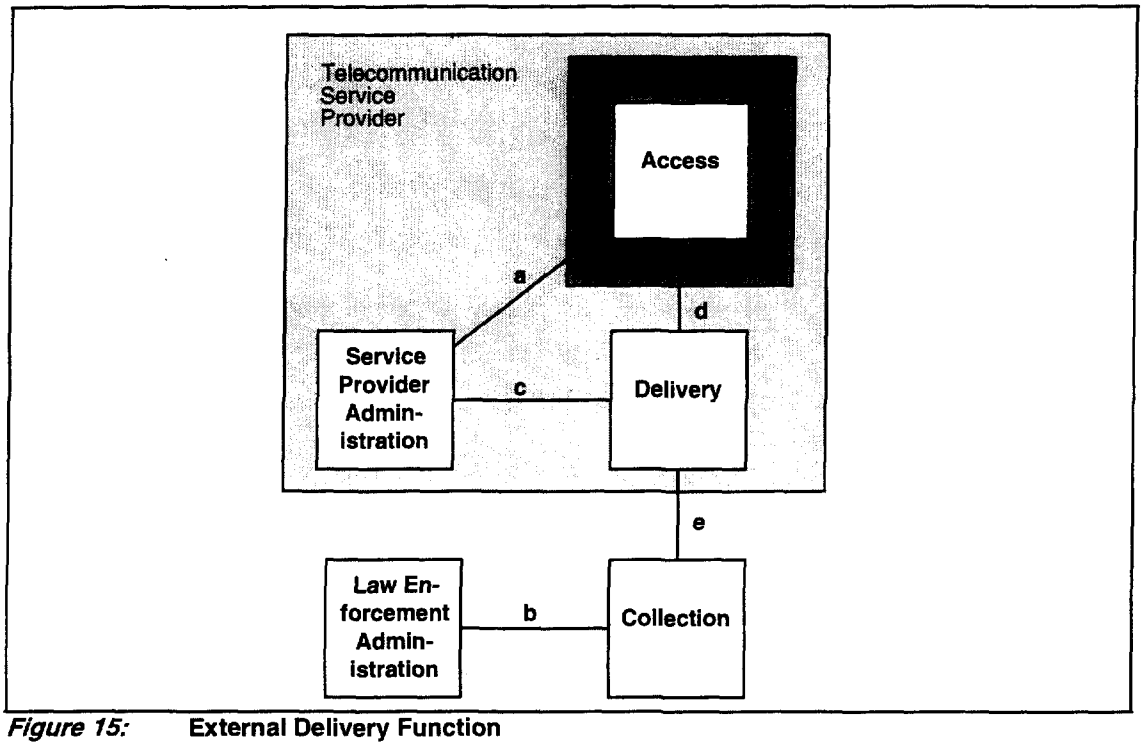

Figure 15: **External Delivery Function**

The Delivery Function may be integrated into the switch itself. There are two basic variations on this theme dealing with how separate and distinct the administration interfaces remain. These are shown in Figure 16 and Figure 17.

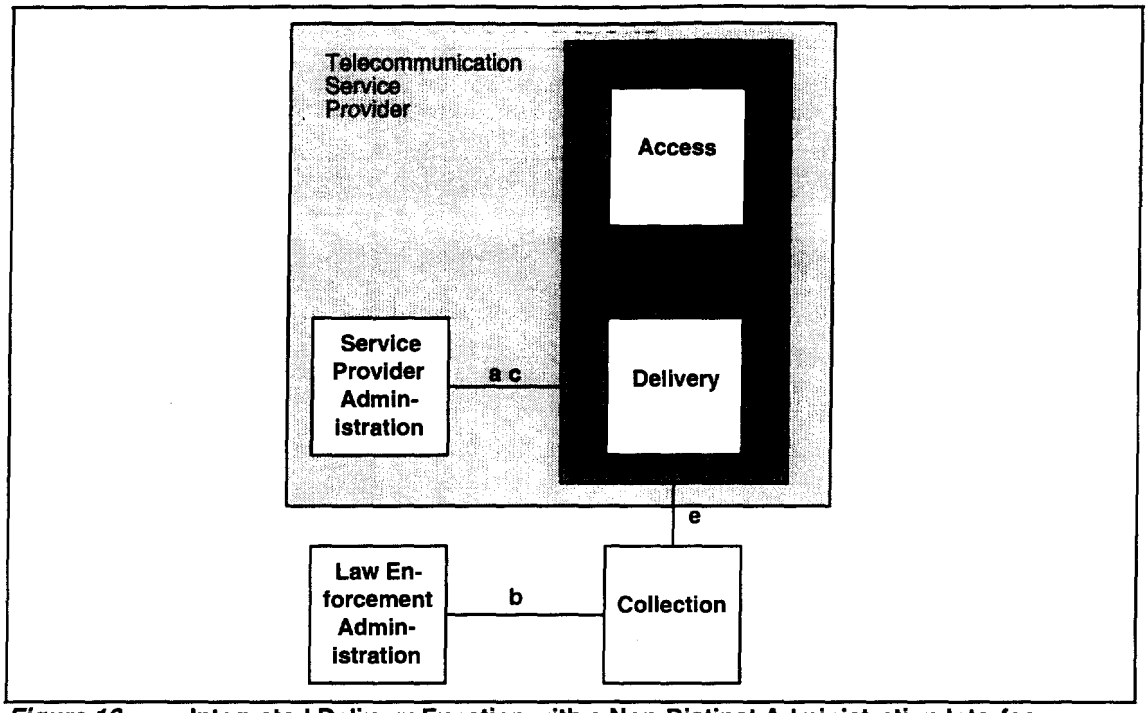

Figure 16: **Integrated Delivery Function with a Non-Distinct Administration Interface**

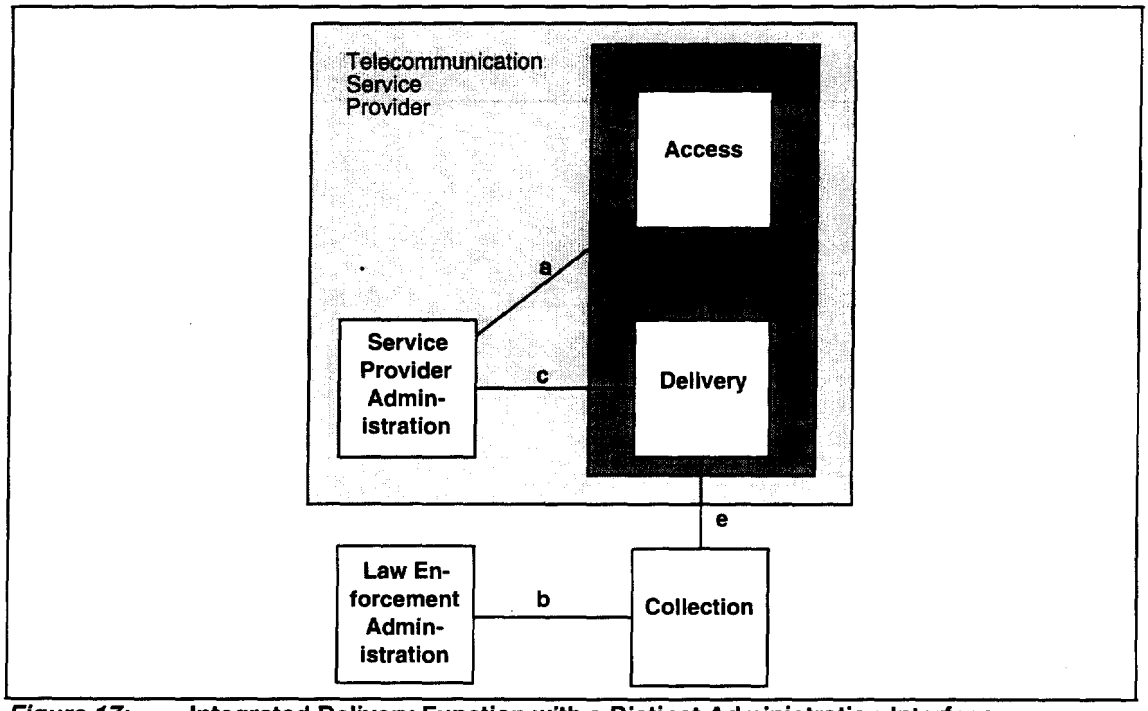

Figure 17: **Integrated Delivery Function with a Distinct Administration Interface**